52. A data processing system which has the ability to deal with infection of a file with a virus, the system comprising:

a storage device storing files;

a virus scanner detecting if a file stored in said storage device is infected with a virus; and

a saving unit saving a detected virus-infected file into a specific area within said storage device.

53. A data processing system according to claim 52, further comprising a managing unit managing the detected virus-infected file that is saved in the specific area.

54. A data processing system according to claim 53, further comprising a deleting unit deleting the detected virus-infected file.

55. A data processing system according to claim 52, further comprising an encoder unit encrypting the detected virus-infected file.

56. A data processing system according to claim 52, wherein the virus-infected file saved in the specific area is not able to run.

57. A method for dealing with infection of a file by a virus, the method comprising:

storing files;

detecting if a stored file is infected with a virus; and saving a detected virus-infected file into a specific area designated for virus-infected files.

58. A method according to claim 57, further comprising managing the detected virus infected file that is saved in the specific area.

59. A method according to claim 58, further comprising deleting the detected virus-infected file.

60. A method according to claim 57, further comprising encrypting the detected virus infected file that is saved in the specific area.

61. A method according to claim 57, further comprising prohibiting the detected virus-infected file from executing.

62. A computer readable storage controlling a computer to perform a method for dealing with infection of a file by a virus, by:

detecting if a file stored in a storage device is infected with a virus; and

saving a detected virus-infected file into a specific area designated for virus-infected files.

63. A computer readable storage according to claim 62, the method further comprising managing the detected virus-infected file that is saved in the specific area.

64. A computer readable storage according to claim 63, the method further comprising deleting the detected virus-infected file.

65. A computer readable storage according to claim 62, the method further comprising encrypting the detected virus-infected file that is saved in the specific area.

66. A computer readable storage according to claim 62, the method further comprising prohibiting the detected virus-infected file from executing.

67. An apparatus, comprising:

a virus scanner scanning a file stored in a storage device for infection with a virus; and

a quarantining device quarantining the file from non-infected files on the storage device, when the file is infected.

68. An apparatus according to claim 67, wherein the storage device comprises at least one section dedicated to storing infected files.

69. An apparatus according to claim 67, wherein the quarantining device requests a user's permission before performing the quarantining.

70. An apparatus according to claim 67, further comprising an encrypting device encrypting the quarantined file.

71. An apparatus according to claim 67, wherein the file, when infected, is kept in a quarantine area on the storage device.

72. An apparatus, comprising:

a virus scanner scanning a file stored in a storage device for infection with a virus; and

an encrypting device encrypting the file on the storage device, if the file is infected.

73. An apparatus according to claim 72, wherein the file, when encrypted, cannot be executed because of its encrypted state.

74. An apparatus according to claim 72, wherein the encrypting device requests a user's permission before performing the encrypting.

75. An apparatus comprising:

a storage device storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

an input device inputting a selected file with infected status; and

a quarantining device quarantining the selected file on the storage device.

76. An apparatus according to claim 75, wherein the selected file, when quarantined, is unable to be executed.

77. An apparatus according to claim 75, further comprising an encrypting device encrypting the selected file.

78. An apparatus according to claim 75, wherein the quarantining device keeps the selected file in a quarantine area on the storage device.

79. An apparatus, comprising:

a storage device storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

an input device inputting a selected file to be encrypted; and

an encrypting device encrypting the selected file.

80. An apparatus according to claim 79, wherein the selected file, when encrypted, is unable to be executed.

81. A method, comprising:

scanning a file for infection with a virus; and

quarantining the file if infected with a virus.

82. A method according to claim 81, further comprising requesting a users permission before performing the quarantining.

83. A method according to claim 81, wherein the file, when infected, is kept in a quarantine area in the storage device.

84. A method, comprising:

scanning a file for infection with a virus;

quarantining the file from non-infected files if the file is infected with a virus; and

encrypting the file, when infected.

85. A method, comprising:

scanning a file for infection with a virus; and

encrypting the file when infected with a virus.

86. A method according to claim 85, wherein the file, when encrypted, cannot be executed because of its encrypted state.

87. A method according to claim 85, further comprising requesting a users permission before performing the encrypting.

88. A method, comprising:

storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

inputting a selected file with infected status to be quarantined; and

quarantining the selected file.

89. A method according to claim 88, wherein the file, when quarantined, is unable to be executed.

90. A method according to claim 88, further comprising encrypting the selected file, when infected.

91. A method according to claim 88, wherein the file, when quarantined, is kept in a quarantine area in a storage device.

92. A method, comprising:

storing a plurality of files and a status for each file indicating whether the file is infected with a virus;

inputting a selected file to be encrypted; and

encrypting the selected file.

93. A method according to claim 92, wherein the encrypted file is unable to be executed.

94. A computer readable storage controlling a computer by:

scanning a file for infection with a virus; and

quarantining the file if infected with a virus.

95. A computer readable storage according to claim 94, further comprising requesting a users permission before performing the quarantining.

96. A computer readable storage according to claim 94, wherein the file, when quarantined, is kept in a quarantine area in the storage device.

97. A computer readable storage controlling a computer by:

scanning a file for infection with a virus;

quarantining the file from non-infected files, when infected; and

encrypting the file.

98. A computer readable storage controlling a computer by:

scanning a file for infection with a virus; and

encrypting the file when infected with a virus.

99. A computer readable storage according to claim 98, wherein the file, when encrypted, cannot be executed because of its encrypted state.

100. A computer readable storage according to claim 98, further comprising requesting a users permission before performing the encrypting.

101. A computer readable storage controlling a computer by:

storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

inputting a selected file with infected status to be quarantined; and

quarantining the selected file.

102. A computer readable storage according to claim 101, wherein the selected file is unable to be executed.

103. A computer readable storage according to claim 101, further comprising encrypting the selected file.

104. A computer readable storage according to claim 101, wherein the selected file is kept in a quarantine area in the storage device.

105. A computer readable storage controlling a computer by:

storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

inputting a selected file to be encrypted; and

encrypting the selected file.

106. A computer readable storage according to claim 105, wherein the selected file, after encryption, is unable to be executed.

107. A computer readable data structure controlling a computer, comprising:

a list of files stored on a storage device;

a virus status for each of the files indicating whether or not the file is virus infected; and

a quarantine status for each of the files indicated whether or not the file is quarantined.

108. A computer readable data structure controlling a computer, comprising:

a list of files stored on a storage device that are virus-infected; and

a quarantine status for each of the files indicating whether or not the file is quarantined.

109. A method comprising:

scanning a file for infection with a virus; and

isolating the file from non-infected files, if the file is infected with a virus.

110. An apparatus comprising:

a virus scanner detecting if a file is infected with a virus; and

a saving unit saving a detected virus-infected file into a separate storage area for virus infected files.